

Задача №1

В проверочной матрице нет одинаковых столбцов. В этом можно убедиться непосредственно или заметить, что каждый столбец является представлением натуральных чисел от 1 до 15 в двоичной системе счисления. Поэтому любые два столбца линейно независимы (их сумма не равна нулевому столбцу). В тоже время существуют три линейно зависимых столбца. Например, четвёртый и два последних столбца линейно зависимы. Следовательно, линейный групповой код с данной проверочной матрицей имеет кодовое расстояние равное 3. Такое расстояние позволяет исправлять с помощью данного кода одну ошибку.

Задача №2

Многочлен $f(x) = 6 + 4x + 4x^2 + x^3 + x^4 + 3x^5 + x^6$ может быть представлен в виде $f(x) = 5 + (x^4 + x + 1)(x^2 + 3x + 1)$. Поэтому $f(x_1) = f(x_2) = 5$ при подстановке в многочлен корней x_1, x_2 квадратного трехчлена $x^2 + 3x + 1$. Это означает, что шифрование осуществлялось прибавлением к порядковому номеру каждой буквы числа 5 и заменой полученного числа соответствующей буквой (шифр Цезаря со смещением равным 5).

Расшифровывание выполняется вычитанием числа 5 из номера буквы зашифрованного текста с последующей заменой полученного числа соответствующей буквой